

Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol

5 The invention prevents server overload and possible
server crippling due to a flooding of connectionless datagrams
caused by intentional attack or otherwise. In response to a
datagram from a host for a specified port, the number of
datagrams already queued to the port from the host is
determined. If this number exceeds a first threshold, the
datagram is discarded. In the preferred embodiment, the
threshold is determined by multiplying a percentage P by the
number of available queue slots remaining for the port.